Security

- Federal Information Processing Standards, on page 1
- Compliance and Policy Control for File Transfer and Screen Capture, on page 2
- Instant Message Encryption, on page 2

Federal Information Processing Standards

Note
This section applies to Cisco Jabber for Windows only.

The Federal Information Processing Standard (FIPS) 140 is a U.S. and Canadian government standard that specifies security requirements for cryptographic modules. These cryptographic modules include the set of hardware, software, and firmware that implements approved security functions and is contained within the cryptographic boundary.

FIPS requires that all encryption, key exchange, digital signatures, and hash and random number generation functions used within the client are compliant with the FIPS 140.2 requirements for the security of cryptographic modules.

FIPS mode results in the client managing certificates more strictly. Users in FIPS mode may see certificate errors in the client if a certificate for a service expires and they haven't reentered their credentials. Users also see a FIPS icon in their hub window to indicate that the client is running in FIPS mode.

Enable FIPS for Cisco Jabber for Windows

Note
The Screen Share feature is not supported if FIPS mode is enabled.

Cisco Jabber for Windows supports two methods of enabling FIPS:

- Operating system enabled—The Windows operating system is in FIPS mode.
- Cisco Jabber bootstrap setting—Configure the FIPS_MODE installer switch. Cisco Jabber can be in FIPS mode on an operating system that is not FIPS enabled. In this scenario, only connections with non-Windows APIs are in FIPS mode.
Table 1: Cisco Jabber for Windows Setting for FIPS

<table>
<thead>
<tr>
<th>Platform Mode</th>
<th>Bootstrap Setting</th>
<th>Cisco Jabber Client Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>FIPS Enabled</td>
<td>FIPS Enabled</td>
<td>FIPS Enabled—Bootstrap setting.</td>
</tr>
<tr>
<td>FIPS Enabled</td>
<td>FIPS Disabled</td>
<td>FIPS Disabled—Bootstrap setting.</td>
</tr>
<tr>
<td>FIPS Enabled</td>
<td>No setting</td>
<td>FIPS Enabled—Platform setting.</td>
</tr>
<tr>
<td>FIPS Disabled</td>
<td>FIPS Enabled</td>
<td>FIPS Enabled—Bootstrap setting.</td>
</tr>
<tr>
<td>FIPS Disabled</td>
<td>FIPS Disabled</td>
<td>FIPS Disabled—Bootstrap setting.</td>
</tr>
<tr>
<td>FIPS Disabled</td>
<td>No setting</td>
<td>FIPS Disabled—Platform setting.</td>
</tr>
</tbody>
</table>

Note
Jabber Voicemail service only accepts TLS Version TLS 1.2 for HTTPS request https://164.62.224.15/vmrest/version with FIPS enabled during an SSL connection.

Compliance and Policy Control for File Transfer and Screen Capture

If you send file transfers and screen captures using the Managed file transfer option on Cisco Unified Communications Manager IM and Presence 10.5(2) or later, you can send the files to a compliance server for audit and policy enforcement.

For more information about compliance, see the Instant Messaging Compliance for IM and Presence Service on Cisco Unified Communications Manager guide.

For more information about configuring file transfer and screen capture, see the Cisco Unified Communications Manager IM and Presence Deployment and Installation Guide.

Instant Message Encryption

Cisco Jabber uses Transport Layer Security (TLS) to secure Extensible Messaging and Presence Protocol (XMPP) traffic over the network between the client and server. Cisco Jabber encrypts point to point instant messages.

On-Premises Encryption

The following table summarizes the details for instant message encryption in on-premises deployments.
Server and Client Negotiation

The following servers negotiate TLS encryption with Cisco Jabber using X.509 public key infrastructure (PKI) certificates with the following:

- Cisco Unified Communications Manager IM and Presence
- Cisco Unified Communications Manager

After the server and client negotiate TLS encryption, both the client and server generate and exchange session keys to encrypt instant messaging traffic.

The following table lists the PKI certificate key lengths for Cisco Unified Communications Manager IM and Presence Service.

<table>
<thead>
<tr>
<th>Version</th>
<th>Key Length</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco Unified Communications Manager IM and Presence Service versions 9.0.1 and higher</td>
<td>2048 bit</td>
</tr>
<tr>
<td>Cisco Unified Presence version 8.6.4</td>
<td>2048 bit</td>
</tr>
<tr>
<td>Cisco Unified Presence versions lower than 8.6.4</td>
<td>1024 bit</td>
</tr>
</tbody>
</table>

XMPP Encryption

Cisco Unified Communications Manager IM and Presence Service uses 256-bit length session keys that are encrypted with the AES algorithm to secure instant message traffic between Cisco Jabber and the presence server.

If you require additional security for traffic between server nodes, you can configure XMPP security settings on Cisco Unified Communications Manager IM and Presence Service. See the following for more information about security settings:

- Cisco Unified Presence—Configuring Security on Cisco Unified Presence
- Cisco Unified Communications Manager IM and Presence Service—Security configuration on IM and Presence

Instant Message Logging

You can log and archive instant messages for compliance with regulatory guidelines. To log instant messages, you either configure an external database or integrate with a third-party compliance server. Cisco Unified Communications Manager IM and Presence Service does not encrypt instant messages that you log in external databases or in third party compliance servers. You must configure your external database or third party compliance server as appropriate to protect the instant messages that you log.

See the following for more information about compliance:
Cloud-Based Encryption

The following table summarizes the details for instant message encryption in cloud-based deployments:

<table>
<thead>
<tr>
<th>Connection</th>
<th>Protocol</th>
<th>Negotiation Certificate</th>
<th>Expected Encryption Algorithm</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client to server</td>
<td>XMPP within TLS</td>
<td>X.509 public key infrastructure certificate</td>
<td>AES 128 bit</td>
</tr>
<tr>
<td>Client to client</td>
<td>XMPP within TLS</td>
<td>X.509 public key infrastructure certificate</td>
<td>AES 256 bit</td>
</tr>
</tbody>
</table>

Server and Client Negotiation

The following servers negotiate TLS encryption with Cisco Jabber using X.509 public key infrastructure (PKI) certificates with the Cisco Webex Messenger service.

After the server and client negotiate TLS encryption, both the client and server generate and exchange session keys to encrypt instant messaging traffic.

XMPP Encryption

The Cisco Webex Messenger service uses 128-bit session keys that are encrypted with the AES algorithm to secure instant message traffic between Cisco Jabber and the Cisco Webex Messenger service.

You can optionally enable 256-bit client-to-client AES encryption to secure the traffic between clients.

Instant Message Logging

The Cisco Webex Messenger service can log instant messages, but it does not archive those instant messages in an encrypted format. However, the Cisco Webex Messenger service uses stringent data center security, including SAE-16 and ISO-27001 audits, to protect the instant messages that it logs.

The Cisco Webex Messenger service cannot log instant messages if you enable AES 256 bit client-to-client encryption.

For more information about encryption levels and cryptographic algorithms, including symmetric key algorithms such as AES or public key algorithms such as RSA, see Next Generation Encryption at this link https://www.cisco.com/c/en/us/about/security-center/next-generation-cryptography.html.

For more information about X.509 public key infrastructure certificates, see the Internet X.509 Public Key Infrastructure Certificate and CRL Profile document at this link https://www.ietf.org/rfc/rfc2459.txt.
Client-to-Client Encryption

By default, instant messaging traffic between the client and the Cisco WebEx Messenger service is secure. You can optionally specify policies in the Cisco WebEx Administration Tool to secure instant messaging traffic between clients.

The following policies specify client-to-client encryption of instant messages:

- **Support AES Encoding For IM**—Sending clients encrypt instant messages with the AES 256-bit algorithm. Receiving clients decrypt instant messages.

- **Support No Encoding For IM**—Clients can send and receive instant messages to and from other clients that do not support encryption.

The following table describes the different combinations that you can set with these policies.

<table>
<thead>
<tr>
<th>Policy Combination</th>
<th>Client-to-Client Encryption</th>
<th>When the Remote Client Supports AES Encryption</th>
<th>When the Remote Client Does not Support AES Encryption</th>
</tr>
</thead>
</table>
| Support AES Encoding For IM = false  
Support No Encoding For IM = true | No | Cisco Jabber sends unencrypted instant messages.  
Cisco Jabber does not negotiate a key exchange. As a result, other clients do not send Cisco Jabber encrypted instant messages. | Cisco Jabber sends and receives unencrypted instant messages. |
| Support AES Encoding For IM = true  
Support No Encoding For IM = true | Yes | Cisco Jabber sends and receives encrypted instant messages.  
Cisco Jabber displays an icon to indicate instant messages are encrypted. | Cisco Jabber sends encrypted instant messages.  
Cisco Jabber receives unencrypted instant messages. |
| Support AES Encoding For IM = true  
Support No Encoding For IM = false | Yes | Cisco Jabber sends and receives encrypted instant messages.  
Cisco Jabber displays an icon to indicate instant messages are encrypted. | Cisco Jabber does not send or receive instant messages to the remote client.  
Cisco Jabber displays an error message when users attempt to send instant messages to the remote client. |

---

**Note**

Cisco Jabber does not support client-to-client encryption with group chats. Cisco Jabber uses client-to-client encryption for point-to-point chats only.
For more information about encryption and Cisco WebEx policies, see *About Encryption Levels* in the Cisco WebEx documentation.

**Encryption Icons**

Review the icons that the client displays to indicate encryption levels.

**Lock Icon for Client to Server Encryption**

In both on-premises and cloud-based deployments, Cisco Jabber displays the following icon to indicate client to server encryption:

![Lock Icon](image)

**Padlock Icon for Client to Client Encryption**

In cloud-based deployments, Cisco Jabber displays the following icon to indicate client to client encryption:

![Padlock Icon](image)

**Local Chat History**

Chat history is retained after participants close the chat window and until participants sign out. If you do not want to retain chat history after participants close the chat window, set the Disable_IM_History parameter to true. This parameter is available to all clients except IM-only users.

For on-premises deployment of Cisco Jabber for Mac, if you select the **Save chat archives to:** option in the **Chat Preferences** window of Cisco Jabber for Mac, chat history is stored locally in the Mac file system and can be searched using Spotlight.

Cisco Jabber does not encrypt archived instant messages when local chat history is enabled.

For mobile clients, you can disable local chat history if you do not want unencrypted instant messages to be stored locally.

For desktop clients, you can restrict access to chat history by saving archives to the following directories:

- **Windows**: `%USERPROFILE%\AppData\Local\Cisco\Unified Communications\Jabber\CSF\History\uri.db`
- **Mac**:`~/Library/Application Support/Cisco/Unified Communications/Jabber/CSF/History/uri.db`